

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

KEONNE RODRIGUEZ and
WILLIAM LONERGAN HILL,

Defendants.

SUPERSEDING INDICTMENT

S3 24 Cr. 82 (RMB)

COUNT ONE

(Conspiracy to Commit Money Laundering)

The Grand Jury charges:

OVERVIEW

1. From at least in or about 2015 through at least in or about April 2024, in the Southern District of New York and elsewhere, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, developed, marketed, and operated a cryptocurrency mixing service known as Samourai Wallet (“Samourai”). While offering Samourai as a “privacy” service, the defendants intended for Samourai to be a haven for criminals to engage in large-scale money laundering and sanctions evasion. Indeed, as the defendants intended and well knew, a substantial portion of the funds that Samourai processed were criminal proceeds passed through Samourai for purposes of concealment. Through the defendants’ mixing service, they earned millions of dollars in fees by laundering the proceeds of drug trafficking, darkweb marketplaces, cyber intrusions and frauds, and other criminal activities. In total, Samourai laundered at least \$250 million dollars of criminal proceeds during the relevant period.

2. At all times relevant to this Indictment, KEONNE RODRIGUEZ, the defendant, was a Co-Founder and Chief Executive Officer of Samourai. RODRIGUEZ is a United States citizen who at all relevant times resided in either Florida, Pennsylvania, or the United Kingdom.

3. At all times relevant to this Indictment, WILLIAM LONERGAN HILL, the defendant, was a Co-Founder and Chief Technology Officer for Samourai. HILL is a United States citizen who at all relevant times resided in France or Portugal.

Background on Bitcoin

4. “Cryptocurrency,” also known as “digital currency,” is a digital representation of value that can be traded, and functions as a medium of exchange, a unit of account, and a store of value.

5. Bitcoin (“BTC”) is a type of cryptocurrency. Bitcoins are not issued by a government, bank, or company, but rather are electronically generated, transacted, and tracked through computer software operating on a decentralized “peer-to-peer” network.

6. Bitcoins can typically be acquired by purchasing them from a Bitcoin “exchange.” An individual can also acquire Bitcoin through “mining,” which is the way new Bitcoin is produced and the way Bitcoin transactions are verified.

7. When a user acquires Bitcoins, the Bitcoins are sent to the user’s Bitcoin “address,” analogous to a bank account number, which is designated by a string of letters and numbers. The user can then conduct transactions with other Bitcoin users by transferring Bitcoins to their Bitcoin addresses via the Internet. To authorize a transfer of Bitcoins from an address, a user must use his or her “private key,” or password, to conduct the Bitcoin transaction. A user may have multiple Bitcoin addresses and corresponding private keys, which are frequently stored in a user’s Bitcoin “wallet.”

8. All transfers of Bitcoins between different Bitcoin addresses are recorded on a public online ledger known as the “Blockchain.”

Background on Samourai

9. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, began developing Samourai in or about 2015. RODRIGUEZ and HILL owned, controlled, managed, and supervised Samourai, which was engaged in the business of transferring funds, in the form of Bitcoin, on behalf of the public. The purpose of Samourai was to conceal the source of Bitcoin transactions and the individuals who owned the Bitcoin, in exchange for substantial fees. Samourai operated a mobile application that users could download onto their cellphones, and the application has been downloaded over 100,000 times. After users downloaded Samourai, they could store their private keys for any BTC addresses they controlled inside of the Samourai program. These private keys were not shared with Samourai employees, but as further discussed below, Samourai operated a centralized coordinator server (the “Coordinator Server”), managed by RODRIGUEZ and HILL, that, among other things, supervised, executed, and facilitated transactions between Samourai users, and to do so, Samourai created new BTC addresses to which Samourai sent users’ BTC. Samourai was used by customers all over the world, including customers located in the United States and in the Southern District of New York.

10. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, designed Samourai to offer at least two features intended to assist individuals engaged in criminal conduct to conceal the source of the proceeds of their criminal activities: First, Samourai offered a cryptocurrency mixing service known as “Whirlpool,” which coordinated and mixed batches of cryptocurrency exchanges between groups of Samourai users to prevent tracing of criminal proceeds by law enforcement on the Blockchain. Second, Samourai offered a service called

“Ricochet,” during which a Samourai user chose to send Bitcoin to another Bitcoin address and Samourai created additional and unnecessary intermediate transactions (known as “hops”), thus sending the user’s Bitcoin to additional Bitcoin addresses created by Samourai through layered transactions before delivering the user’s Bitcoin to the destination address designated by the user. This feature similarly could be used to prevent law enforcement and/or cryptocurrency exchanges from recognizing that a particular batch of cryptocurrency originates from criminal activity. From the start of the Whirlpool service in or about 2019, and of the Ricochet service in or about 2017, at least 80,000 BTC (worth over \$2 billion applying the BTC-USD conversion rates at the time of each transaction) passed through these two services operated by Samourai. Samourai collected a fee for both services, estimated to be at least \$3.4 million for Whirlpool transactions and \$1.1 million for Ricochet transactions through May 2023.

11. In addition, to conceal the source of the Bitcoin and the owners of the Bitcoin, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, intentionally did not require Samourai customers to provide “know your customer” or “KYC” information to Samourai. RODRIGUEZ and HILL advertised and promoted the fact that Samourai’s customers could use the Whirlpool or Ricochet functions without providing any identifying information to Samourai. As discussed below, this deliberate decision not to implement KYC encouraged and enabled its customers to engage in transactions meant to conceal the nature, location, source, ownership, and control of criminal proceeds by making those transactions more difficult to trace.

12. Indeed, as is described below, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, specifically promoted Samourai for its ability to allow customers to engage in anonymous transactions. For example, in the Twitter message below,

HILL touted the fact that Samourai had no KYC and no terms and conditions (“T&C”) governing the use of Samourai:

TDevD [No KYC, no T&C, no] @SamouraiDev

13. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, also promoted Samourai’s lack of KYC procedures on Samourai’s website. For example, Samourai’s website promoted Samourai as a “modern bitcoin wallet hand forged to keep your transactions private your identity masked and your funds secured.” Samourai claimed that its application allowed users to “[b]e your own Swiss Bank . . . No email address, no ID checks, and no hassle.”

14. At all relevant times, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, exercised control over Samourai, including arranging for the payment of necessary expenses—including web hosting services and fees to the Google Play Store—to allow Samourai to be available to users, including in the United States.

Background on Whirlpool

15. To use the “Whirlpool” feature, which was introduced by Samourai in or around April 2019, a Samourai user selected an amount of BTC that they wished to mix and the pool in which they wanted to mix that BTC. Each pool was designed to accept BTC in a set increment and a flat fee to contribute BTC to the pool. Samourai offered up to four different pools, with denominations of approximately 0.001 BTC, 0.01 BTC, 0.05 BTC, and 0.5 BTC.¹ As of April 2024, the fees for each of the pools was as follows:

¹ These pool sizes are approximate, as the exact denominations of BTC inputs include mining fees that are necessary to broadcast transactions to the blockchain. So for example, the exact amount of an input into the 0.001 BTC pool could be 0.001000302 BTC.

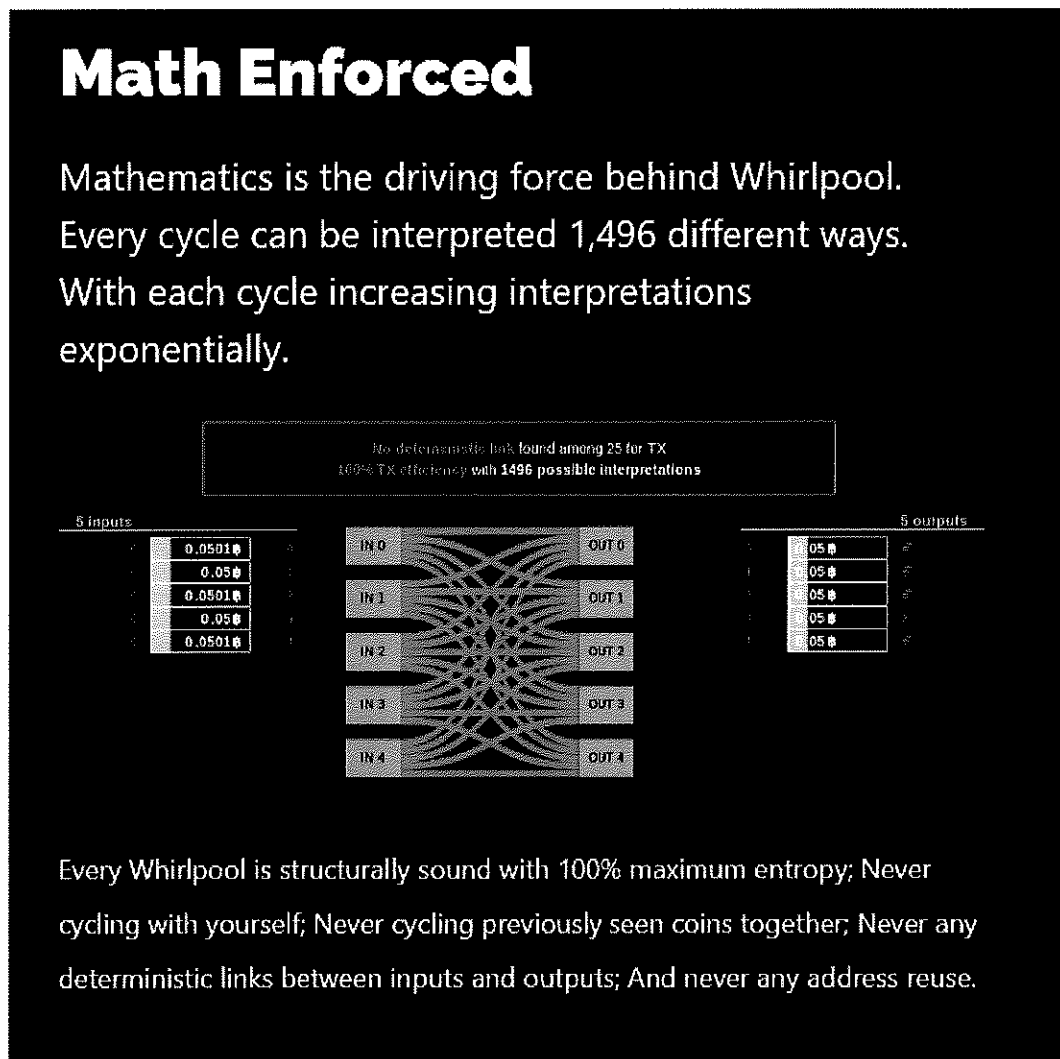
Pool	Pool Fee
0.001 BTC	0.00005 BTC
0.01 BTC	0.0005 BTC
0.05 BTC	0.00175 BTC
0.5 BTC	0.0175 BTC

16. The “Whirlpool” feature functioned as follows:

a. First, once a user contributed cryptocurrency from their Samourai wallet to be sent into the Whirlpool, Samourai “cut down” the cryptocurrency into the correct sizes for a chosen pool. Samourai also collected its fee and the mining fees from the transaction, and then the funds waited to join a mix. For example, if a user wished to contribute 1 BTC into the 0.05 BTC pool, the Samourai software on the user’s cellphone broadcast a transaction to the blockchain transferring 1 BTC into 19 addresses, each containing approximately 0.05 BTC (plus the mining fees necessary for broadcasting the subsequent transactions to the blockchain). Each of these 19 addresses containing approximately 0.05 BTC served as an “input” in a Whirlpool transaction. Additionally, the broadcasted transaction sent Samourai’s fees from the user to an address designated by the Samourai software. Samourai returned back to the user any leftover funds from this transaction that were too small to enter the Whirlpool by replacing them in a separate address.

b. Second, through the Coordinator Server that Samourai operated, the Samourai application on a user’s cellphone communicated with other Samourai users, and Samourai’s Coordinator Server randomly selected four other inputs already in the selected pool to be mixed with the new incoming input and communicated that information to each user. The Samourai application on each user’s cellphone then broadcasted a transaction to the Blockchain in

which all five inputs (each a separate address) were then transferred to five outputs (each a separate address). Samourai's Coordinator Server automatically generated the new addresses that were used as inputs and outputs throughout the process on behalf of the users, although the private keys for these cryptocurrency addresses were stored in each user's individual cellphone and not shared with Samourai's employees. Below is a graphical representation posted on Samourai's website of the five input and five output transaction:



If, for example, as set forth above, 1 BTC entered the 0.05 BTC pool, Samourai combined each new unit of 0.05 BTC contributed by the user into the 0.05 BTC pool with four other units of 0.05

BTC already in the pool from up to four other users to engage in a five-input-five-output transaction.

c. Finally, after the mix was complete, Samourai continued to automatically mix the outputs with other batches of cryptocurrency that were in the same pool indefinitely as new cryptocurrency entered the pool, until a user chose to remove their cryptocurrency from the Whirlpool. In other words, each time a transaction in the Whirlpool occurred, one new input and four old inputs already in a pool would engage in a five-input-five-output transaction. All of these transactions were coordinated by Samourai's Coordinator Server. Samourai incentivized users to keep their cryptocurrency in the Whirlpool (and therefore generate additional liquidity in the pool) by making subsequent remixes free. Mining fees for the broadcasting of these cryptocurrency transactions were covered by new BTC inputs entering the pool. Samourai's Whirlpool feature generated over \$3 million in fees for Samourai—the large majority of which were also stored in the Whirlpool as a source of additional liquidity.

Background on Ricochet

17. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, caused the Samourai website to tout the fact that its Ricochet feature could assist customers in further obfuscating the link between customers' deposits and withdrawals. In particular, the Samourai website described the Ricochet feature as a "premium tool that adds extra hops of history to your transaction" and would allow customers to "[s]tump the blacklists and help guard against unjust 3rd party account closures."² RODRIGUEZ and HILL designed the "Ricochet" feature to

² "Blacklists" are lists of cryptocurrency addresses known to be associated with sanctioned entities and known criminal activity frequently used by cryptocurrency exchanges to block particular transactions from occurring. For example, the United States Treasury Department's Office of Foreign Asset Controls maintains lists of cryptocurrency addresses known to be linked to criminal activities or other threats to the national security, foreign policy, or economy of the United States.

build in additional and unnecessary intermediate transactions (known as “hops”) on behalf of Samourai users in order to further obscure the source and ownership of funds when Samourai users sent cryptocurrency from one address to another address.

18. To use the Ricochet feature, which was introduced by Samourai in or around 2017, a Samourai user selected an amount of BTC that they wished to send, and the destination address where it was to be sent. The user could also decide whether they wanted the Ricochet transaction to occur instantly or spread out over a designated amount of time. Samourai’s Coordinator Server provided an address where Samourai’s fees were received prior to the execution of the series of Ricochet transactions. The Samourai application then created the series of BTC transactions for each Ricochet, including the creation of new addresses, which were transmitted to Samourai’s Coordinator Server. Samourai’s Coordinator Server was responsible for broadcasting the Ricochet transactions to the BTC network. As with the Whirlpool feature, Samourai automatically generated the new cryptocurrency addresses that were used for these transactions, although the private keys for these addresses were stored in each user’s individual cellphone and not shared with Samourai’s employees. Samourai’s Ricochet feature generated at least \$1 million in fees for Samourai—the large majority of which were then laundered through Samourai’s Whirlpool feature. From Whirlpool and Ricochet, RODRIGUEZ and HILL earned at least \$4 million in fees.

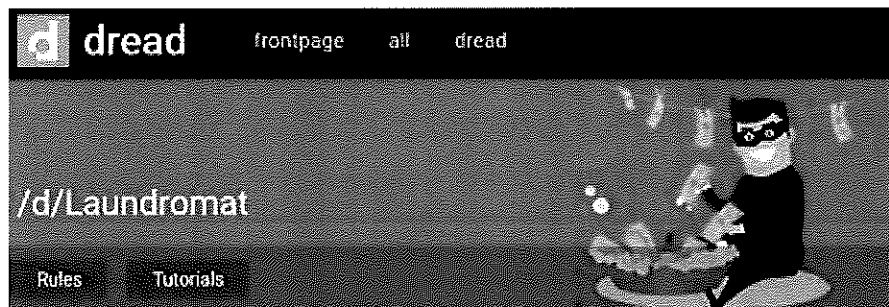
RODRIGUEZ and HILL’s Knew and Intended for Criminal Proceeds to Be Laundered by Samourai


19. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, designed Samourai in whole and in part for the purpose of being used by criminals, actively encouraged and solicited hackers, darknet marketplace users, sanctions evaders, and other criminals to engage in money laundering transactions using Samourai Wallet, and knew that such criminals were in fact using Samourai Wallet to engage in money laundering on Samourai.

Samourai’s commercial success was driven in large part by such transactions, as over \$250 million in crime proceeds were laundered through Samourai.

20. As one example, on or about January 5, 2018, in a WhatsApp chat, when asked by an associate what “mixing”—*i.e.*, what Samourai did and advertised itself as doing—was, KEONNE RODRIGUEZ, the defendant, described that it was “money laundering for bitcoin.” In other words, RODRIGUEZ admitted that the Samourai mixing service was a *money laundering* service, the crime he is charged with conspiring to commit in Count One of this Indictment. Rodriguez’s associate then responded with an emoji: “🤖.”

21. As another example, on Dread, a Reddit-like dark web message board featuring discussions about darknet marketplaces, WILLIAM LONERGAN HILL, the defendant, expressly advertised Samourai as a money laundering service. As pictured below, the discussion occurred in the subforum titled “Laundromat,” bearing the banner photograph of a masked criminal washing money in a bathtub (*i.e.*, laundering or cleaning his dirty money), and in a post titled “How to clean dirty BTC.”



 **How to clean dirty BTC?**

In this forum, a Dread user asked what were the most “[s]ecure methods to clean dirty BTC” so that the BTC would become “untraceable, clean” and the Dread user would “never get caught.” On or about October 2, 2023, HILL responded by criticizing a competitor mixer (“Mixer-1”) by directing the Dread user to “Avoid [Mixer-1] at all costs” and, instead, encouraged the Dread user

to use Samourai, writing that “Samourai Whirlpool is a much better option” to clean dirty BTC—or, in other words, to launder money.

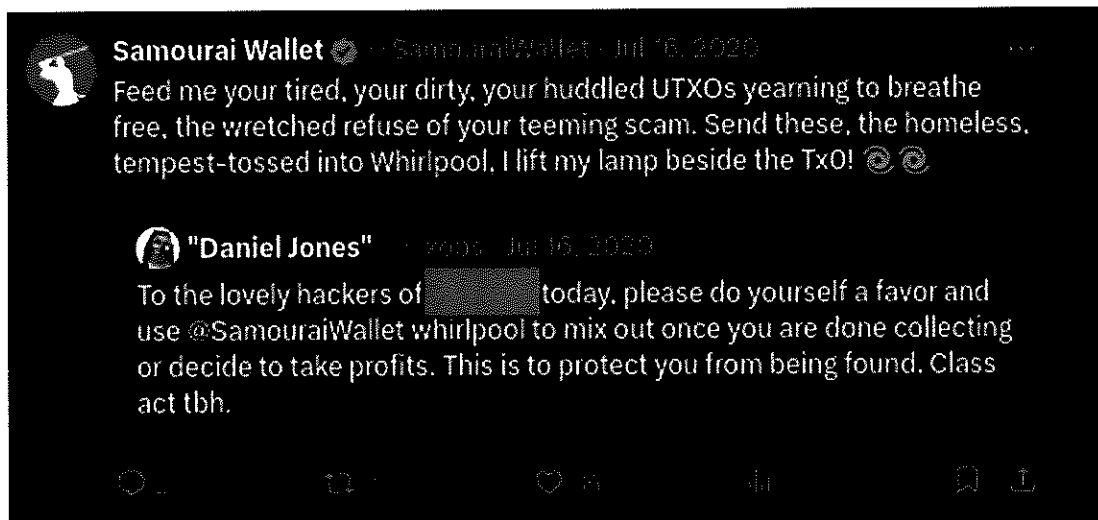
22. In another Dread post, WILLIAM LONERGAN HILL, the defendant, again encouraged darknet marketplace customers to use Samourai to conceal their crimes. In a discussion thread in the subforum “DarkNetMarkets,” titled “Payments on darknet markets,” a Dread user asked why darknet marketplaces still allowed BTC for transactions when “Bitcoin is a well know[n] traceable tool, LE [*i.e.*, law enforcement] have proved it time and time again,” and expressing concern that “people are buying drugs here playing with their freedom.” On or about November 14, 2020, HILL responded by criticizing Mixer-1, directing the Dread user to “avoid[]” Mixer-1 “at all costs,” and, encouraging the Dread user to use Samourai Whirlpool.

23. KEONNE RODRIGUEZ, the defendant, was well aware that WILLIAM LONERGAN HILL, the defendant, advertised Samourai specifically on dark web message boards, including Dread, because on or about August 18, 2020, RODRIGUEZ stated in a Telegram thread with an associate that “we’re making a space on the dark net boards, dread in particular” and HILL “has been doin[g] a lot of work there.”

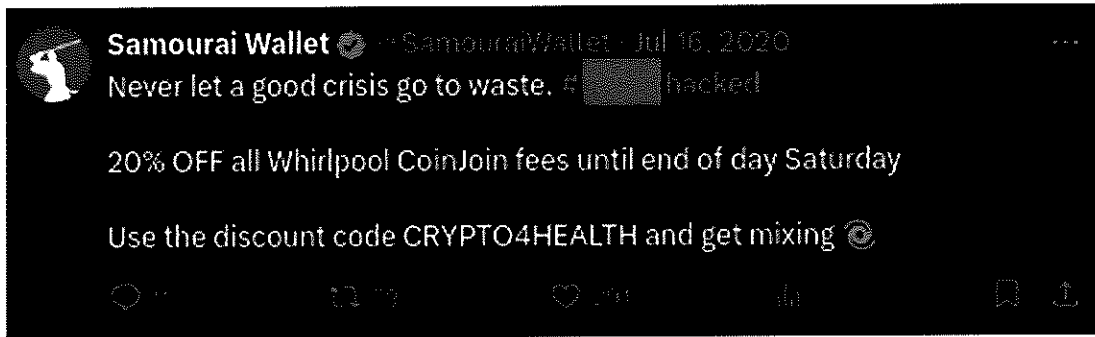
24. In private Telegram messages with an associate, KEONNE RODRIGUEZ, the defendant, made clear that he intended for criminals to use Samourai to conceal their crime proceeds and that he believed that Samourai’s competitor, Mixer-1, inadequately concealed crime proceeds, which likely would result in incarceration. For example, on or about July 27, 2019, RODRIGUEZ wrote that Mixer-1 was “playing fast and loose” with its concealment methodology, and “is likely to get someone locked up.” RODRIGUEZ’s associate replied, “[e]specially as some of the people that have BTC from obvious hacks etc haven’t mixed them in a sophisticated way.” RODRIGUEZ endorsed the message by responding, “yeah it is crazy.”

25. In or about June 2020, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, tracked in real time the flow of crime proceeds of a well-publicized hack of a prominent social media company (“Social Media Company-1”), and both publicly and privately expressed their intent and desire that the hackers use Samourai’s Whirlpool service (and not its competitor Mixer-1) to launder the crime proceeds of the hack of Social Media Company-1 or else the hackers would risk incarceration.

a. As pictured below, in a tweet on or about July 16, 2020, after a third party encouraged the “lovely hackers of [Social Media Company-1]” to “use @SamouraiWallet whirlpool to mix out once you are done collecting or decide to take profits” in order to “protect you from being found,” RODRIGUEZ responded by personally encouraging the [Social Media Company-1] hackers to “[f]eed” and “[s]end” the crime proceeds into “Whirlpool.”

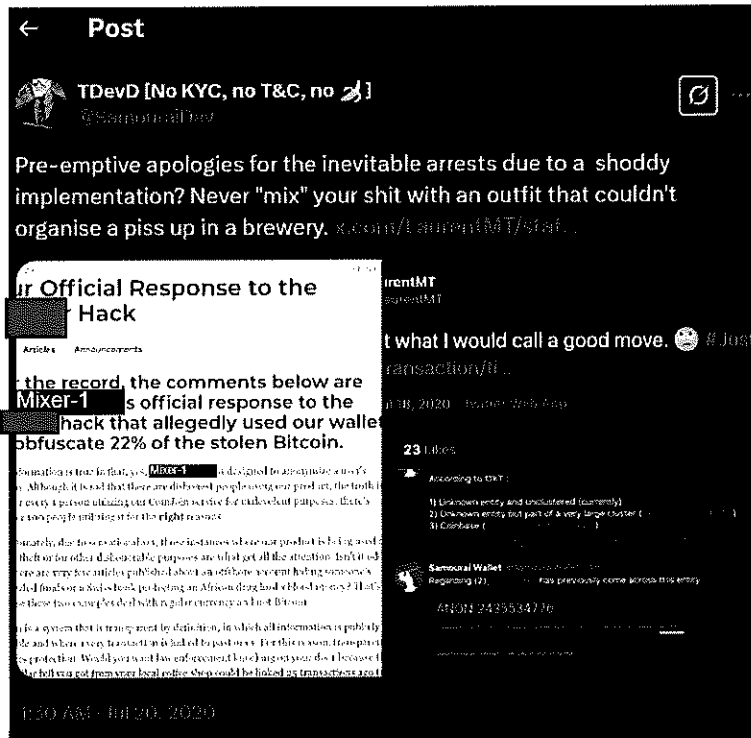


b. Later that same day, RODRIGUEZ tweeted the following:



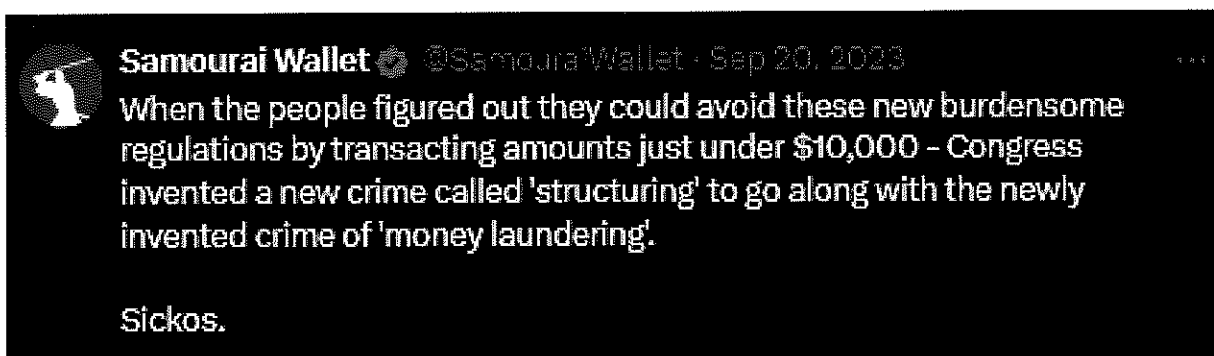
c. The next day, on or about July 17, 2020, in private Telegram messages, an associate complained about the [Social Media Company-1] hackers using Mixer-1 and not Samourai, writing “the hackers will get caught – 100%” and musing, “why oh why can’t someone high profile use Whirlpool?! I know it isn’t necessary but that wou[l]d be so cool.” RODRIGUEZ responded, “We were aware of them entering [Mixer-1] 6 hours ago . . . trust me, we’re all disappointed.” In the ensuing days, RODRIGUEZ and the associate continued to monitor the movement of the Social Media Company-1 hack crime proceeds. Three days later, on or about July 20, 2020, RODRIGUEZ observed that the hackers, in using Mixer-1 and not Samourai to conceal their crime, “are behaving like they want to be caught.”

d. In response to a public statement by Mixer-1 expressing remorse that the Social Media Company-1 hackers used Mixer-1 to launder crime proceeds, on or about July 20, 2020, HILL criticized Mixer-1 both for its apology and for its inadequate concealment of the crime proceeds, which he predicted would lead to “inevitable arrests”:



HILL posted this critique from his Samurai Twitter account, thereby advertising Samurai as a service better able to conceal crime proceeds and prevent detection by law enforcement.

26. On or about September 20, 2023, KEONNE RODRIGUEZ, the defendant, expressed his knowledge of and lack of respect for federal criminal money laundering laws (*i.e.*, the crime he is charged with conspiring to commit in Count One of this Indictment). Specifically, in response to a third party's tweet criticizing legal requirements triggered when a transaction exceeds \$10,000, RODRIGUEZ explained that as a response to market participants circumventing these requirements by structuring their activities to fall just below the \$10,000 reporting threshold:



27. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, operated Twitter accounts that encouraged and openly invited users to launder criminal proceeds through Samourai. For example, in or around June 2022, Samourai’s Twitter account—operated by RODRIGUEZ—posted the following message regarding Russian oligarchs seeking to circumvent sanctions:



28. In a tweet on or about December 12, 2020, KEONNE RODRIGUEZ, the defendant, actively encouraged and solicited sanctions evaders, writing “Users in Iran should run their BTC acquired via Iranian exchanges in Whirlpool.” Moreover, in a tweet on or about September 1, 2019, RODRIGUEZ confirmed that Iran was the second largest country by Samourai Wallet downloads after the United States.



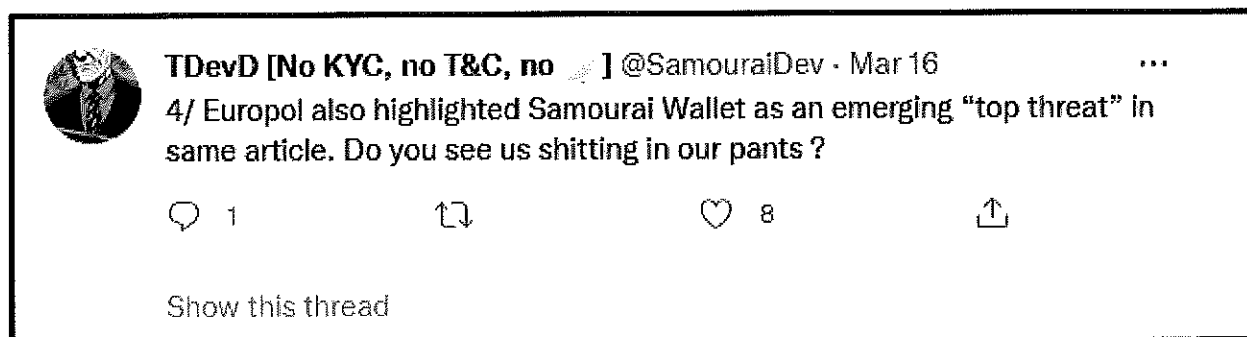
29. Further, in a tweet on or about February 10, 2022, WILLIAM LONERGAN HILL, the defendant, criticized Samourai’s competitor Mixer-1 for inadequately concealing the proceeds of criminal activity: the crime proceeds from a theft from a cryptocurrency exchange in 2016. HILL reposted an image tracing the crime proceeds from the theft into Mixer-1 and wrote that users should “never use” Mixer-1 to do Samourai’s “job”—in other words, concealing crime proceeds.

30. Similarly, in a private message on or about August 27, 2020, WILLIAM LONERGAN HILL, the defendant—using a Twitter account with the username “Samourai Dev”—discussed the use of Samourai by criminals operating in online black markets such as Silk Road in private messages with another Twitter user (the “Twitter User”) (emphasis added):

Twitter User: Silk Road is why I first found Bitcoin and the desire to keep engaging in those types of markets is one reason that I want to defend/strengthen those use cases . . .

Samourai Dev: No, not at all. We probably have different views on some basic tenets of bitcoin, you and I – so to each his own so to speak. At Samourai we are entirely focused on the censorship resistance and black/grey circular economy. This implies no foreseeable mass adoption, although black/grey markets have already started to expand during covid and will continue to do so post-covid. . . .

31. Additionally, in response to Europol highlighting Samourai as a “top threat” to the ability of law enforcement to trace the proceeds of criminal activity, WILLIAM LONERGAN HILL, the defendant, posted a message in or around March 2021 suggesting that Samourai would not change its practices in response to allegations that Samourai was being used for money laundering:



32. Similarly, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, possessed and transmitted to potential investors marketing materials, such as those excerpted below, that discussed how Samourai’s customer base was intended to include criminals seeking privacy or the subversion of safeguards and reporting requirements by financial institutions. For example, in the below excerpt from Samourai’s marketing materials, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, similarly acknowledged that the individuals most likely to use a service like Samourai (“Who is willing to pay for privacy?”) include individuals engaged in criminal activities, including “Restricted Markets.”

Who is willing to pay for privacy?

Online Gambling	\$28.54 B - global market value. <i>SoftSwiss Platform</i> - \$10m / month Largest % of on-chain transaction volume
Restricted Markets	\$237.25 M - amount transacted in 2014
Asset Protection	\$1.5 B - amount held in the top 100 bitcoin addresses

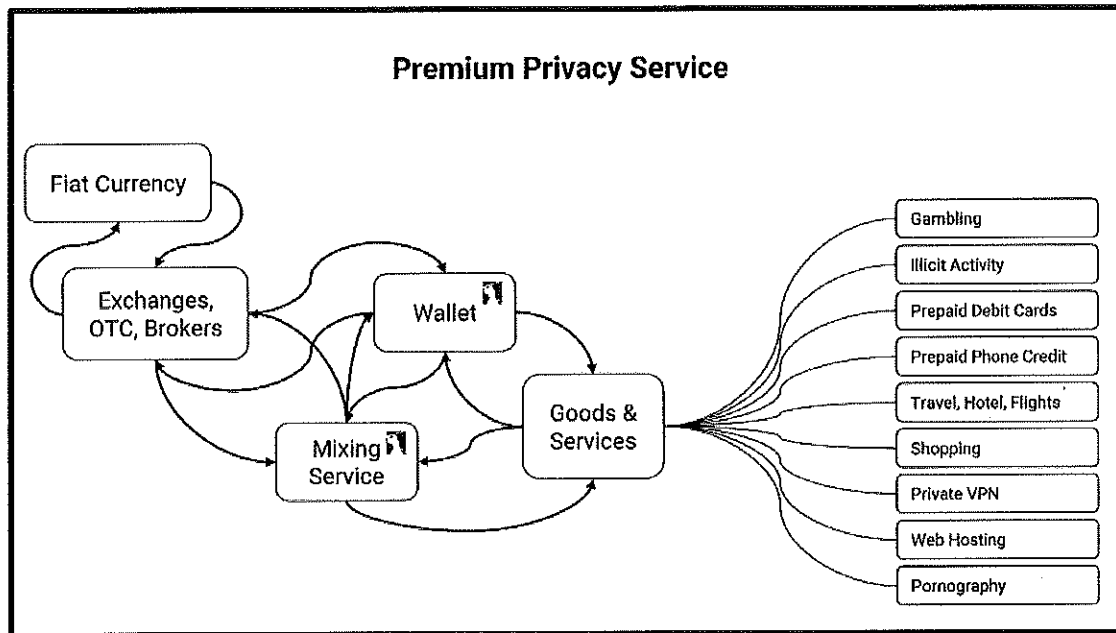
33. In the below excerpt from Samourai's marketing materials, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, acknowledged that its revenues will be derived from "Dark/Grey Market participants" seeking to "swap their bitcoins with multiple parties" to avoid law enforcement detection:

Revenue

Samourai Premium Add Ons

Online Gamblers	On Demand Swap
Dark/Grey Market participants	Users can swap their bitcoins with multiple parties to destroy the metadata that has been created.
Ultra High Net Worth Individuals	0.1% of the amount transacted + 0.0005 BTC flat fee
Asset Protection/Capital Flight	User Monthly Value <i>Assumption: 2 Swaps of 1.00 BTC a month: £7.80</i>

34. In the below excerpt from Samurai's marketing materials, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, promoted Samurai's Wallet and its "Mixing Service" as a "Premium Privacy Service" for transactions involving the proceeds of goods and services that include, among other things, "Illicit Activity":



35. During the arrest of KEONNE RODRIGUEZ, the defendant, in or about April 2024, law enforcement recovered a detailed, six-page handwritten plan for RODRIGUEZ to flee the United States if law enforcement shut down Samurai or planned to arrest the defendants. Among other things, RODRIGUEZ's escape plan set forth that: (a) he planned to travel with multiple passports, a minimum of \$10,000 cash, a burner phone, an unused SIM card, an encrypted USB drive, and a burner laptop; (b) he planned to destroy evidence of Samurai's operations; (c) RODRIGUEZ planned to drive from Pennsylvania to Florida, making sure to evade detection by driving "OFF HIGHWAY," staying in "CASH MOTELS," and paying in "CASH ONLY"; (d) from there, RODRIGUEZ would then take a boat to Jamaica ("HIRE BOAT & CAPTAIN TO GO BY SEA") and potentially fly from Jamaica to Cuba or from Jamaica to the United Kingdom; (e)

RODRIGUEZ contemplated travelling to meet WILLIAM LONERGAN HILL, the defendant; (f) RODRIGUEZ planned to use a United Kingdom passport while fleeing from law enforcement; (g) RODRIGUEZ detailed multiple “STASH” houses in Florida and Pennsylvania where he planned to store burner phones; and (h) RODRIGUEZ planned to use a storage unit registered in someone else’s name that is part of a “LOCAL, NON FRANCHISE” company, and considered paying for it “IN CASH.”

Samourai Was a Vehicle for Money Laundering

36. KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, intended the Whirlpool and Ricochet features to enable Samourai users to launder criminal proceeds by concealing the criminal source of the funds and making it difficult for law enforcement to trace the funds to their illicit source. Because Samourai provided its customers with a method to engage in transactions and move funds on the BTC blockchain in ways that prevented tracing on the public blockchain, not all of the funds passing through the Samourai Whirlpool and Ricochet can be attributed to particular actors. However, at a minimum, at least \$250 million in criminal proceeds were laundered through the Samourai Whirlpool and Ricochet services between its launch in or about 2015 and in or about December 2023.

37. WILLIAM LONERGAN HILL, the defendant, knew in real time that hack crime proceeds were flowing through Samourai. Three days after a well-publicized, \$26 million hack of a decentralized cryptocurrency exchange (“Crypto Exchange-1”), in private Telegram messages, HILL and an associate discussed how hack proceeds were flowing through Samourai. On or about February 19, 2024, HILL and the associate had the following discussion:

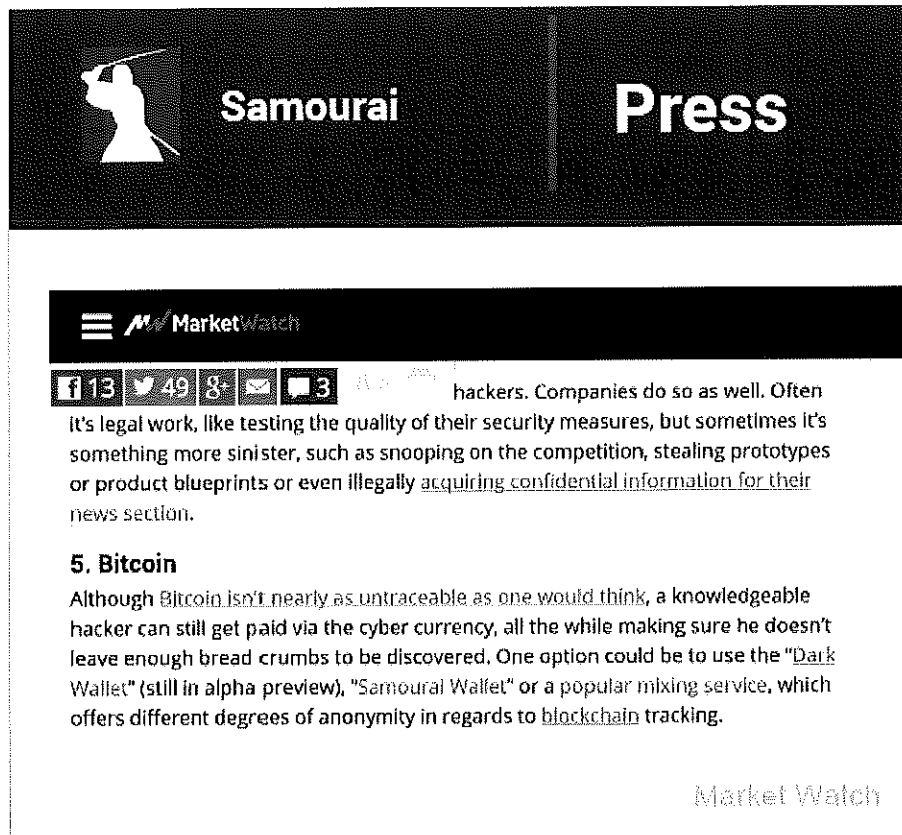
HILL: Not sure if you are using 0.5 pool right now but liquidity in that pool is very high as of 72 hours ago

Associate: [Crypto Exchange-1] hacker sent a lot of funds in your pool, they constantly remixing

That's why

HILL: anyway, I'll keep and I [*i.e.*, 'an eye'] on it. Thanks for reaching out

38. Further, on or about September 1, 2015, KEONNE RODRIGUEZ, the defendant, emailed WILLIAM LONERGAN HILL, the defendant, with the subject "LOL," a link to a press report from in or about August 25, 2015, titled "6 'services' that make hackers rich," which specifically referenced Samurai Wallet. The piece noted that "much" of hackers' work "is usually illegal," and "a knowledgeable hacker can still get paid via [Bitcoin], all the while making sure he doesn't leave enough bread crumbs to be discovered. One option could be to use . . . 'Samurai Wallet' or a popular mixing service, which offers different degrees of anonymity in regards to blockchain tracking." On his laptop, RODRIGUEZ excerpted this language from the press report in the below PowerPoint presentation, dated on or about October 15, 2015, in order to promote Samurai.



39. Moreover, KEONNE RODRIGUEZ, the defendant, also possessed on his laptop a Drug Enforcement Administration (“DEA”) document from in or about January 2019, marked “law enforcement sensitive,” describing Samurai Wallet’s likely use by drug trafficking organizations selling drugs in dark web marketplaces.

40. Despite knowing full well that Samurai was being used to launder criminal proceeds, and that Samurai’s Whirlpool and Ricochet features were being used for the purposes of concealing criminal proceeds, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, took no steps to prevent or stop money laundering on Samurai. To the contrary, Samurai has described itself on its website as a group of “privacy activists who have dedicated our lives to creating the software that Silicon Valley will never build, the regulators will never allow, and the VC’s [venture capitalists] will never invest in.”

41. Likewise, in a tweet on or about February 3, 2016, KEONNE RODRIGUEZ, the defendant, made clear that he understood that he risked incarceration because Samourai was flouting anti-money laundering (“AML”) or know your customer (“KYC”) requirements: “We rather sit in a jail cell than comply with KYC/AML requirements for Bitcoin.”

42. The over \$250 million dollars of crime proceeds laundered through Samourai include, among other criminal sources:

a. **Silk Road Darknet Market.** The Silk Road darknet market (“Silk Road”) was a well-known online black market that was in operation from approximately 2011 until 2013 and was used by numerous drug dealers and other unlawful vendors to distribute illegal drugs and other illicit goods and services. As an example, from at least in or about May 2021 up to and including in or about 2023, over 3,000 BTC of crime proceeds from a former Silk Road vendor that sold illegal narcotics was laundered through Samourai.

b. **Hydra Darknet Market.** The Hydra Darknet Market (“Hydra”) was a Russian-language darknet market launched in 2015 that enabled users to buy and sell illegal drugs, fraudulent documents, stolen financial information, and money laundering and mixing services. In 2021, Hydra accounted for an estimated 80% of all darknet market-related cryptocurrency transactions, and since 2015, the marketplace received approximately \$5.2 billion in cryptocurrency. As an example, in or about October 2020, approximately 40 BTC of crime proceeds from Hydra was laundered through Samourai.

c. **February 2024 Hack.** In or about February 2024, a decentralized cryptocurrency exchange was hacked, and approximately 186 BTC of the criminal proceeds was laundered through Samourai.

d. **July 2022 Hack.** In or about July 2022, a decentralized finance protocol was hacked, and approximately 55 BTC of the criminal proceeds was laundered through Samourai.

e. **November 2022 Hack.** In or about November 2022, a cryptocurrency exchange was hacked, and approximately 389 BTC of the criminal proceeds was laundered through Samourai.

f. **December 2021 Hack.** In or about December 2021, a decentralized finance platform was hacked, and approximately 2,000 BTC of the criminal proceeds was laundered through Samourai.

g. **February 2022 Hack.** In or about February 2022, a web server was hacked, including the exfiltration of a customer database, and approximately 70 BTC of the criminal proceeds was laundered through Samourai.

h. **October 2021 Hack and Spear Phishing Scheme.** In or about October 2021, a spear phishing scheme led to the compromise of the servers of a cloud-service provider and the virtual private server accounts of corporate clients of the cloud-service provider, and approximately 89 BTC of the criminal proceeds was laundered through Samourai.

STATUTORY ALLEGATIONS

43. From at least in or about 2015 up to and including in or about April 2024, in the Southern District of New York and elsewhere, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

44. It was a part and an object of the conspiracy that KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, and others known and unknown, knowing that the

property involved in a financial transaction represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such a financial transaction, which transaction affected interstate and foreign commerce and involved the movement of funds by wire and other means, and which in fact involved the proceeds of specified unlawful activity, to wit, (i) conspiracy to distribute and possess with intent to distribute controlled substances, in violation of Title 21, United States Code, Sections 846 and 841; (ii) wire fraud, in violation of Title 18, United States Code, Section 1343; and (iii) computer fraud and abuse, in violation of Title 18, United States Code, Section 1030, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Section 1956(h).)

COUNT TWO
(Conspiracy to Operate an Unlicensed Money Transmitting Business)

The Grand Jury further charges:

45. The allegations contained in paragraphs 1 through 42 of this Indictment are repeated and realleged as if fully set forth herein.

46. From at least in or about 2015 up to and including in or about April 2024, in the Southern District of New York and elsewhere, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, operation of an unlawful money transmitting business, in violation of Title 18, United States Code, Section 1960(b)(1)(C).

47. It was a part and object of the conspiracy that KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, and others known and unknown, would and did knowingly conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business, which affected interstate and foreign commerce, and otherwise involved the transportation and transmission of funds that were known to the defendants to have been derived from a criminal offense and were intended to be used to promote and support unlawful activity, to wit, RODRIGUEZ and HILL conducted, controlled, managed, supervised, directed, and owned all or part of Samourai, a business that transferred funds on behalf of the public, knowing that the business involved the transportation and transmission of funds that were derived from a criminal offense and were intended to be used to promote and support unlawful activity.

Overt Acts

48. In furtherance of the conspiracy, and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. Between in or around 2015 and in or around April 2024, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, participated in marketing activities on behalf of Samourai to potential customers through social media and email communications, with the knowledge and intent that Samourai would be used for the transportation, transmission, and concealment of funds derived from criminal activity and funds intended to be used to promote and support unlawful activity.

i. For example, on or about June 30, 2022, RODRIGUEZ posted a message on Samourai's Twitter account: "Welcome new Russian oligarch Samourai Wallet users" in response to an article discussing international sanctions on certain Russian oligarchs.

ii. Similarly, on or about March 16, 2020, HILL posted a message on a Twitter account with username @SamouraiDev: "Europol also highlighted Samourai Wallet as an emerging 'top threat' . . . Do you see us shitting in our pants?"

iii. Likewise, on or about October 2, 2023, after a Dread user asked what were the most "[s]ecure methods to clean dirty BTC" so that the BTC would become "untraceable, clean" and the Dread user would "never get caught," HILL responded by directing the Dread user to "Avoid [Mixer-1] at all costs" and, instead, encouraged the Dread user to use Samourai, writing that "Samourai Whirlpool is a much better option"—in other words, that Samourai should be used to launder money.

iv. Further, in a tweet on or about July 16, 2020, after a third party encouraged the "lovely hackers of @[Social Media Company-1]" to "use @SamouraiWallet whirlpool to mix out once you are done collecting or decide to take profits" in order to "protect you from being found," RODRIGUEZ responded by encouraging the Social Media Company-1 hackers to "[f]eed" and "[s]end" the Social Media Company-1 hack crime proceeds into."

b. Between in or around 2015 and in or around April 2024, RODRIGUEZ and HILL participated in the day-to-day operations of Samourai, resulting in Samourai's transport and transfer of funds that were derived from or intended to be used to promote and support a variety of criminal activities, including drug trafficking, darkweb marketplaces, cyber intrusions, and frauds.

(Title 18, United States Code, Section 371.)

FORFEITURE ALLEGATIONS

49. As a result of committing the offenses alleged in Counts One and Two of this Indictment, KEONNE RODRIGUEZ and WILLIAM LONERGAN HILL, the defendants, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any and all property, real and personal, involved in said offenses, or any property traceable to such property, including but not limited to a sum of money in United States currency representing the amount of property involved in said offenses.

Substitute Asset Provision

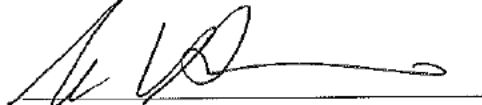
50. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third person;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be subdivided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981 and 982;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)


FOREPERSON


NICOLAS ROOS
Acting Deputy United States Attorney,
Attorney for the United States,
Acting under Authority Conferred by
28 U.S.C. § 515